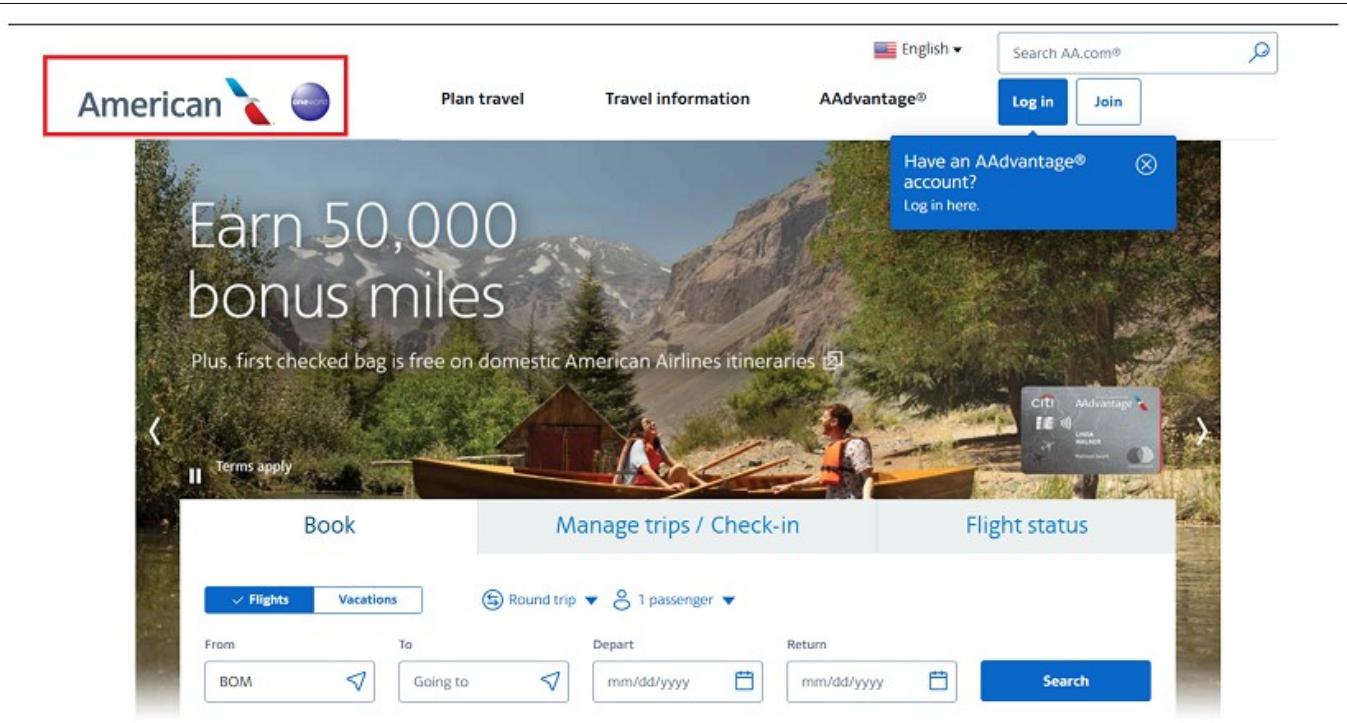
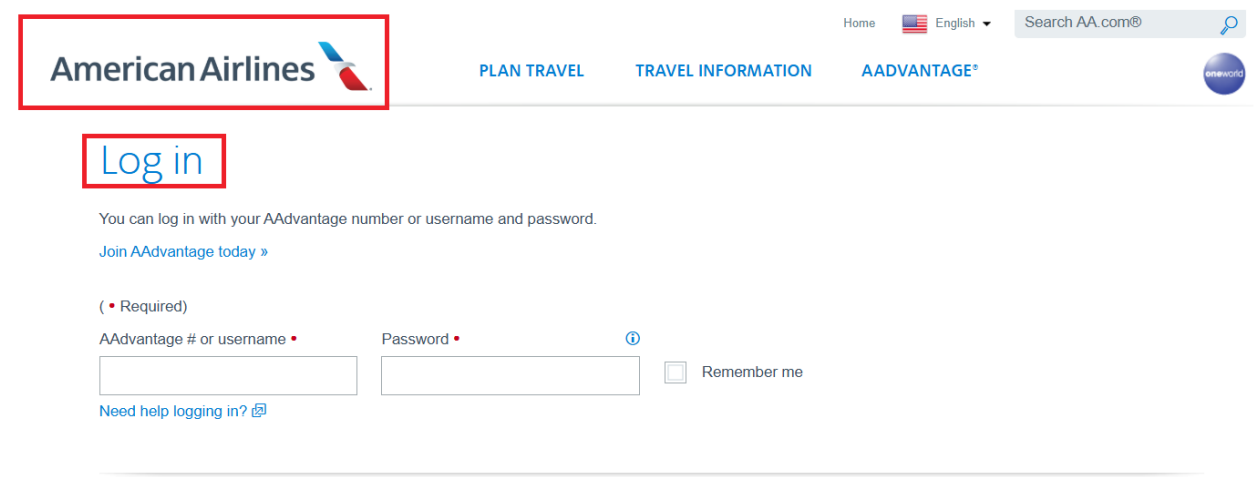
Exhibit 2

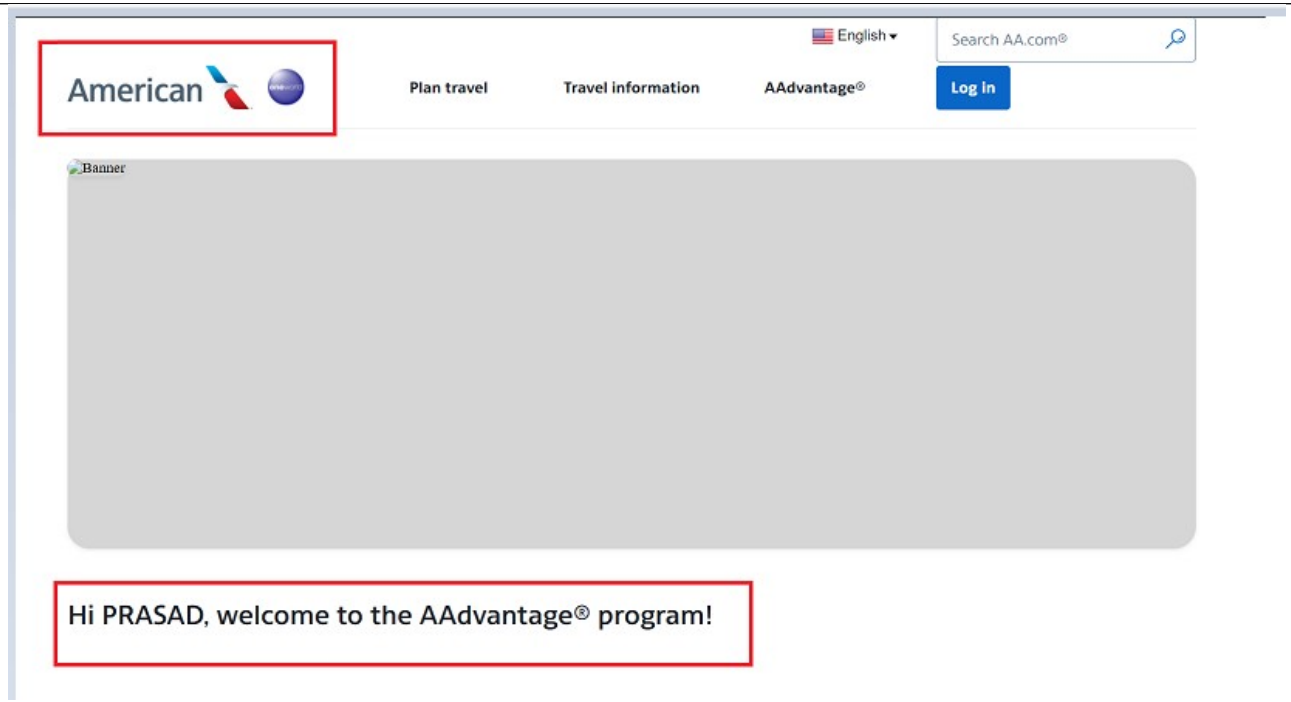
US8677116B1	American Airline's website "aa.com" ("The accused instrumentality")
1. A method of using a computer system to authenticate a user seeking to conduct at least one interaction with a secured capability provided by a computer, the method comprising:	The accused instrumentality practices a method of using a computer system (e.g., authentication server of the accused instrumentality, etc.) to authenticate a user seeking to conduct at least one interaction (e.g., account login, etc.) with a secured capability provided by a computer (e.g., server of the accused instrumentality). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, job searches, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access.



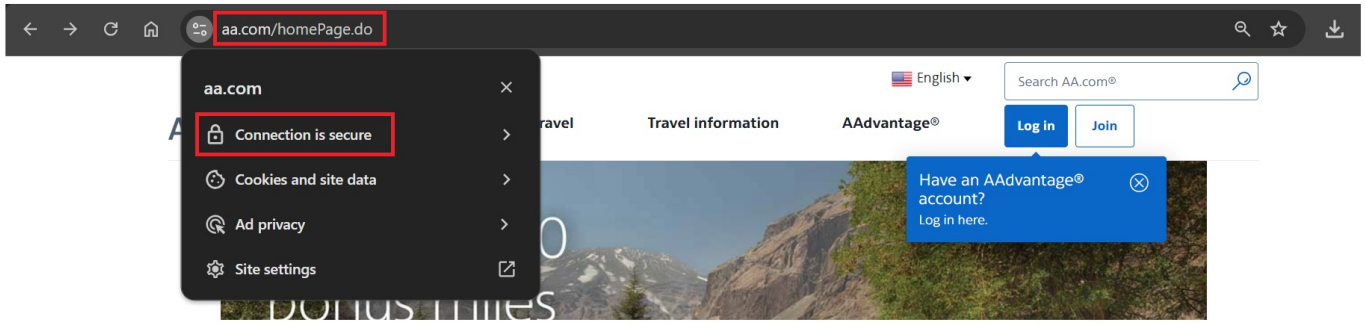
https://www.aa.com/homePage.do



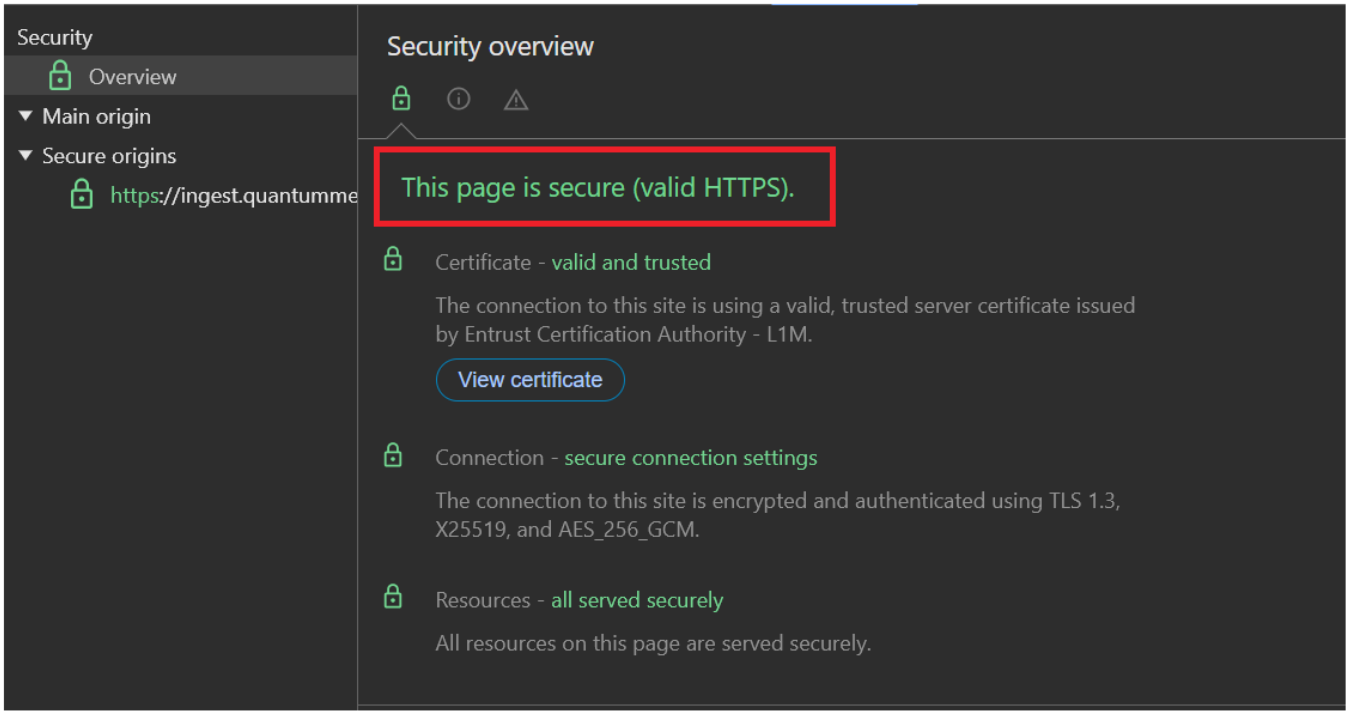
https://www.aa.com/loyalty/login



https://www.aa.com/loyalty/login

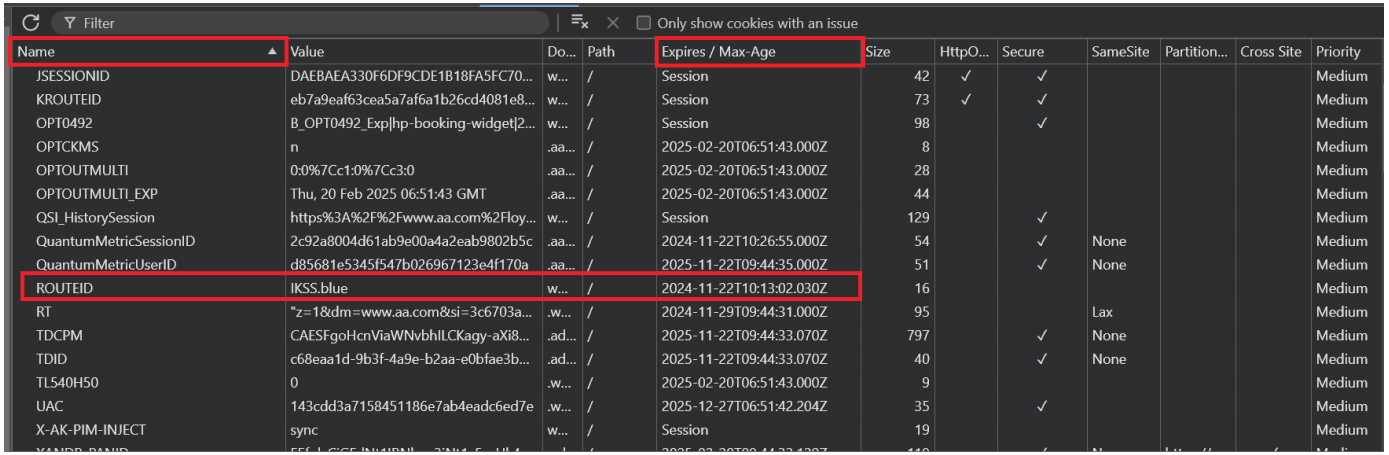


https://www.aa.com/homePage.do

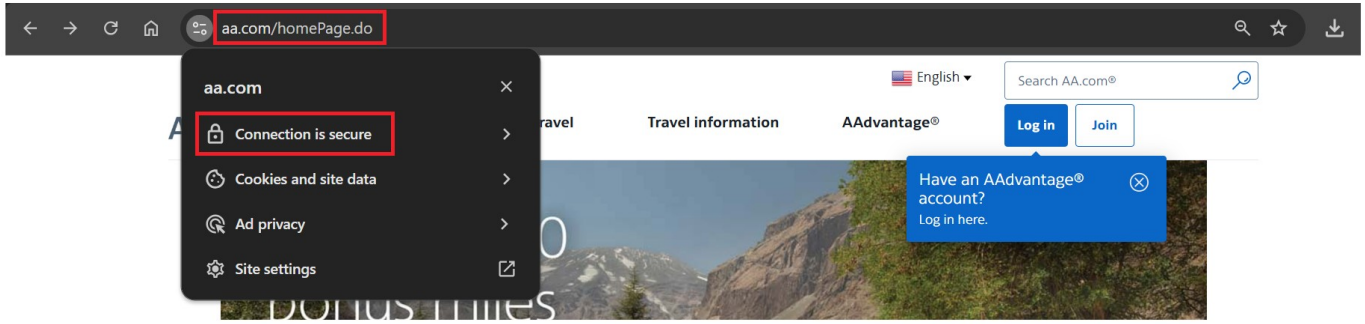


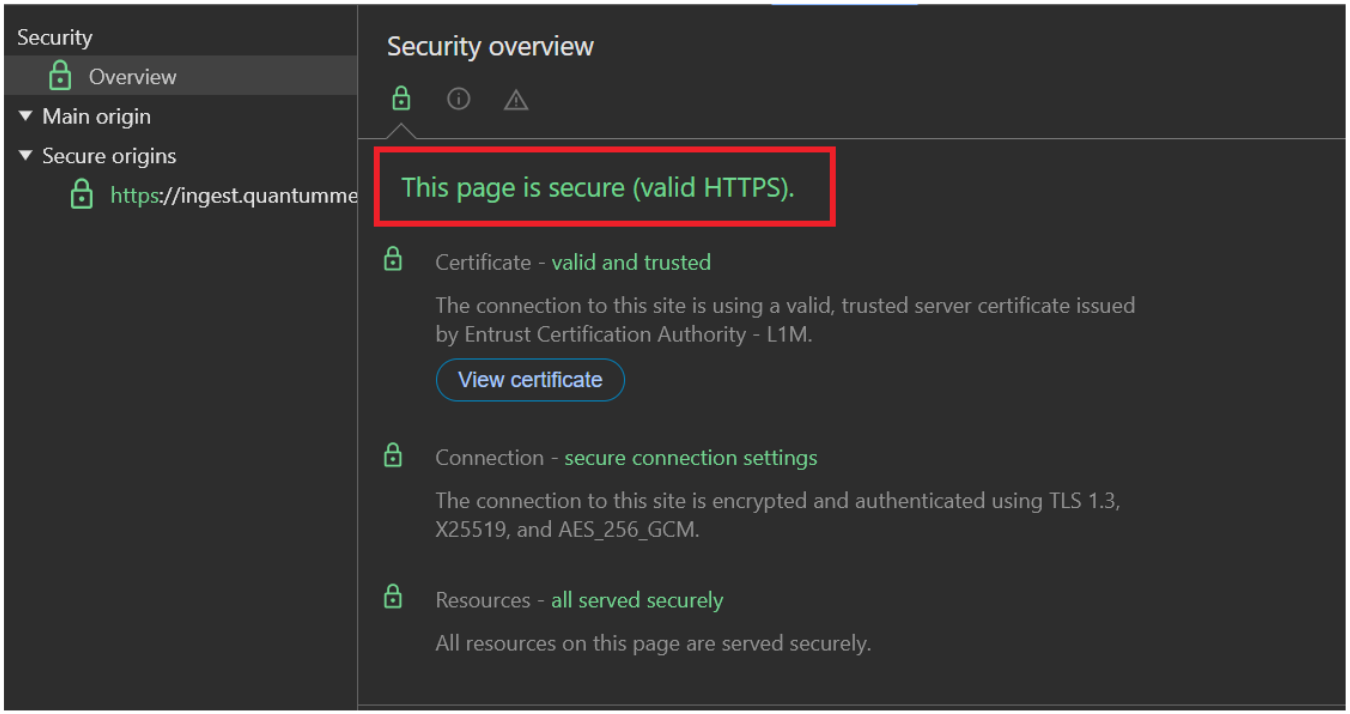
https://www.aa.com/homePage.do

Source: Fiddler capture of the accused instrumentality

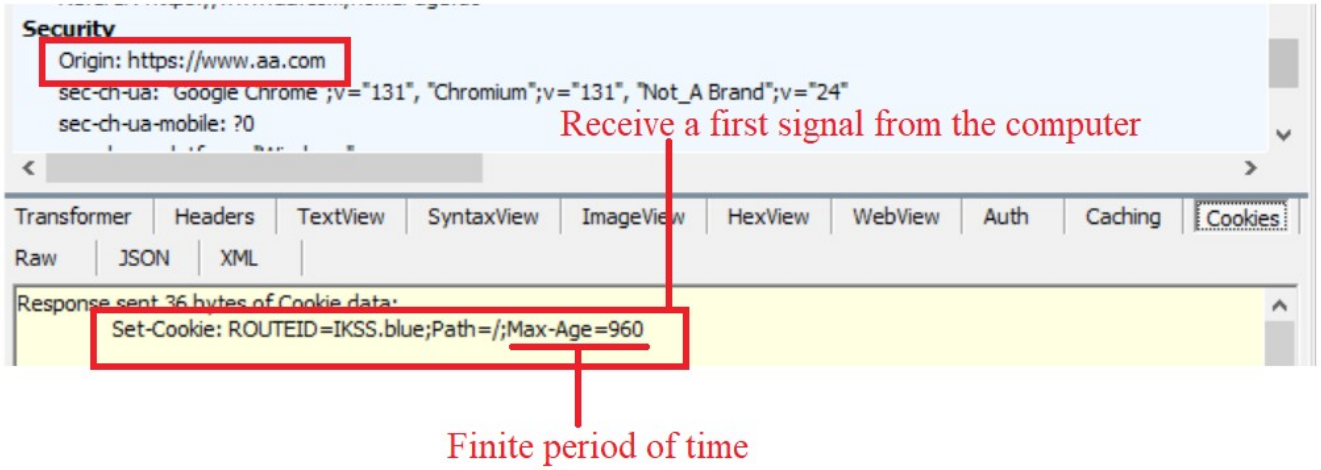


https://www.aa.com/homePage.do

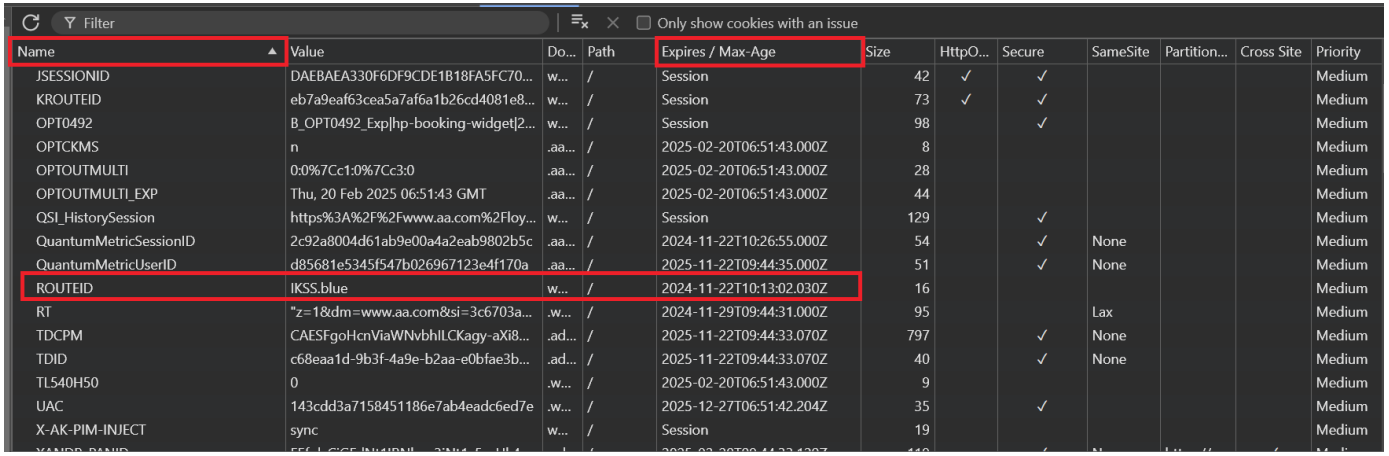
using the computer system to receive a first signal from the computer providing the secured capability, the first signal comprising a reusable identifier corresponding to the secured capability, the reusable identifier assigned for use by the secured capability for a finite period of time;	The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a first signal (e.g., a ROUTEID set response, etc.) from the computer (e.g., server of the accused instrumentality) providing the secured capability (e.g., secure connection with the website, etc.), the first signal comprising a reusable identifier (e.g., ROUTEID, etc.) corresponding to the secured capability (e.g., secure connection with the website, etc.), the reusable identifier assigned for use by the secured capability for a finite period of time (e.g., Max-Age). As shown, the website of the accused instrumentality practices providing secure connection with a user's device (electronic device of the user) through HTTPS connections. This is achieved by an authentication server (a computer system) authenticating users seeking to perform actions such as account login, etc., (interactions) ensuring that interactions with secured features are protected from unauthorized access. The server sends a response to set ROUTEID value, which is set by the user device. As shown, the ROUTEID token set by the end device is reused in all further communications with the server. The ROUTEID token also mentions a Max-Age for the token, indicating that it can be reused for a finite period.  https://www.aa.com/homePage.do



https://www.aa.com/homePage.do



Source: Fiddler captures of the accused instrumentality



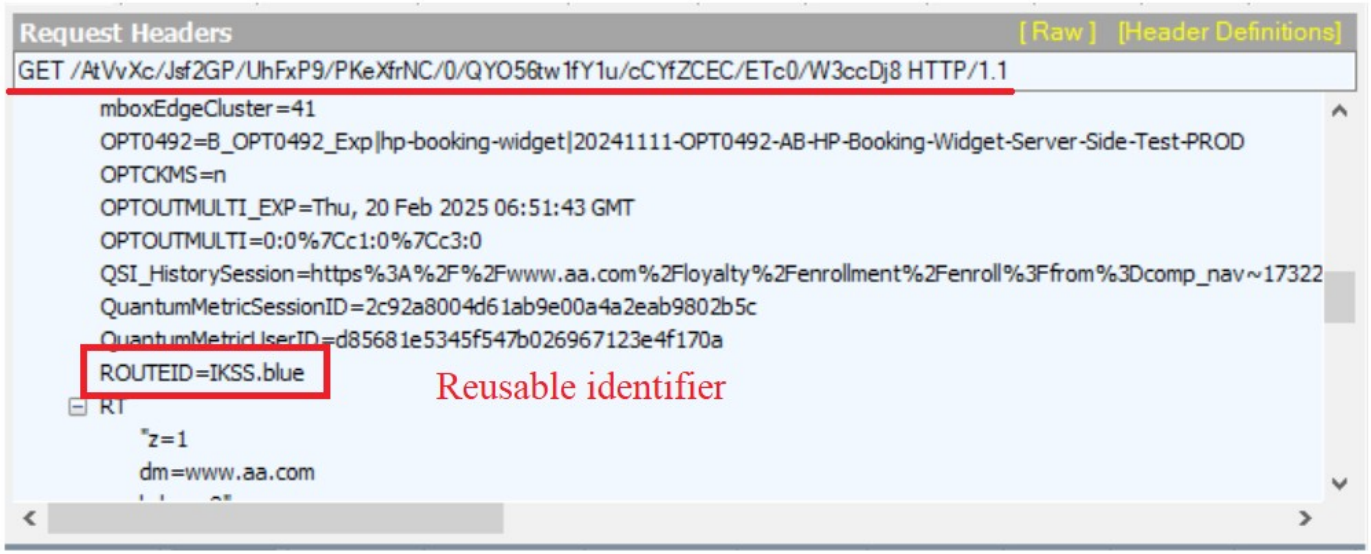
Filter | Only show cookies with an issue

Name	Value	Do...	Path	Expires / Max-Age	Size	HttpO...	Secure	SameSite	Partition...	Cross Site	Priority
JSESSIONID	DAEBAEA330F6DF9CDE1B18FA5FC70...	w...	/	Session	42	✓	✓				Medium
KROUTEID	eb7a9eaf63cea5a7af6a1b26cd4081e8...	w...	/	Session	73	✓	✓				Medium
OPT0492	B_OPT0492_Exp|hp-booking-widget|2...	w...	/	Session	98		✓				Medium
OPTCKMS	n	.aa...	/	2025-02-20T06:51:43.000Z	8						Medium
OPTOUTMULTI	0:0%7Cc1:0%7Cc3:0	.aa...	/	2025-02-20T06:51:43.000Z	28						Medium
OPTOUTMULTI_EXP	Thu, 20 Feb 2025 06:51:43 GMT	.aa...	/	2025-02-20T06:51:43.000Z	44						Medium
QSI_HistorySession	https%3A%2F%2Fwww.aa.com%2Floy...	w...	/	Session	129		✓				Medium
QuantumMetricSessionID	2c92a8004d61ab9e00a4a2eab9802b5c	.aa...	/	2024-11-22T10:26:55.000Z	54		✓	None			Medium
QuantumMetricUserID	d85681e5345f547b026967123e4f170a	.aa...	/	2025-11-22T09:44:35.000Z	51		✓	None			Medium
ROUTEID	IKSS.blue	w...	/	2024-11-22T10:13:02.030Z	16						Medium
RT	"z=1&dm=www.aa.com&si=3c6703a...	.w...	/	2024-11-29T09:44:31.000Z	95			Lax			Medium
TDCPM	CAESFgoHcnViaWNvbhILCKagy-aXi8...	.ad...	/	2025-11-22T09:44:33.070Z	797		✓	None			Medium
TDID	c68eaa1d-9b3f-4a9e-b2aa-e0bfae3b...	.ad...	/	2025-11-22T09:44:33.070Z	40		✓	None			Medium
TL540H50	0	.w...	/	2025-02-20T06:51:43.000Z	9						Medium
UAC	143cdd3a7158451186e7ab4eadc6ed7e	.w...	/	2025-12-27T06:51:42.204Z	35		✓				Medium
X-AK-PIM-INJECT	sync	w...	/	Session	19						Medium

https://www.aa.com/homePage.do

<table>
<tr><td></td><td> 

Source: Fiddler Capture of the accused instrumentality

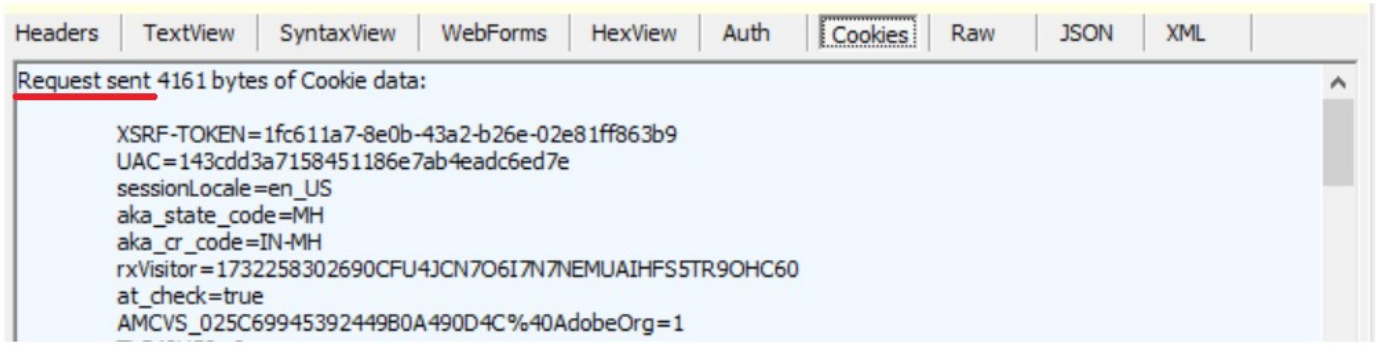


Source: Fiddler Capture of the accused instrumentality</td></tr>
<tr><td>using the computer system to receive a</td><td>The accused instrumentality practices using the computer system (e.g., authentication server of the accused instrumentality, etc.) to receive a second signal</td></tr>
</table>

second signal from an electronic device being used by the user, the second signal comprising a copy of the reusable identifier and user verification information;	(e.g., a request signal from the user device) from an electronic device being used by the user, the second signal (e.g., request signal from the user device) comprising a copy of the reusable identifier (e.g., ROUTEID, etc.) and user verification information (e.g., rxVisitor). When the server sends a message containing an ROUTEID to the user device, the client includes a copy of the ROUTEID in all subsequent requests to the server, along with user verification information (e.g., rxVisitor credentials). This allows the server to authenticate the client for the duration of the session and ensure secure communication between the client and server.  Source: Fiddler Capture of the accused instrumentality

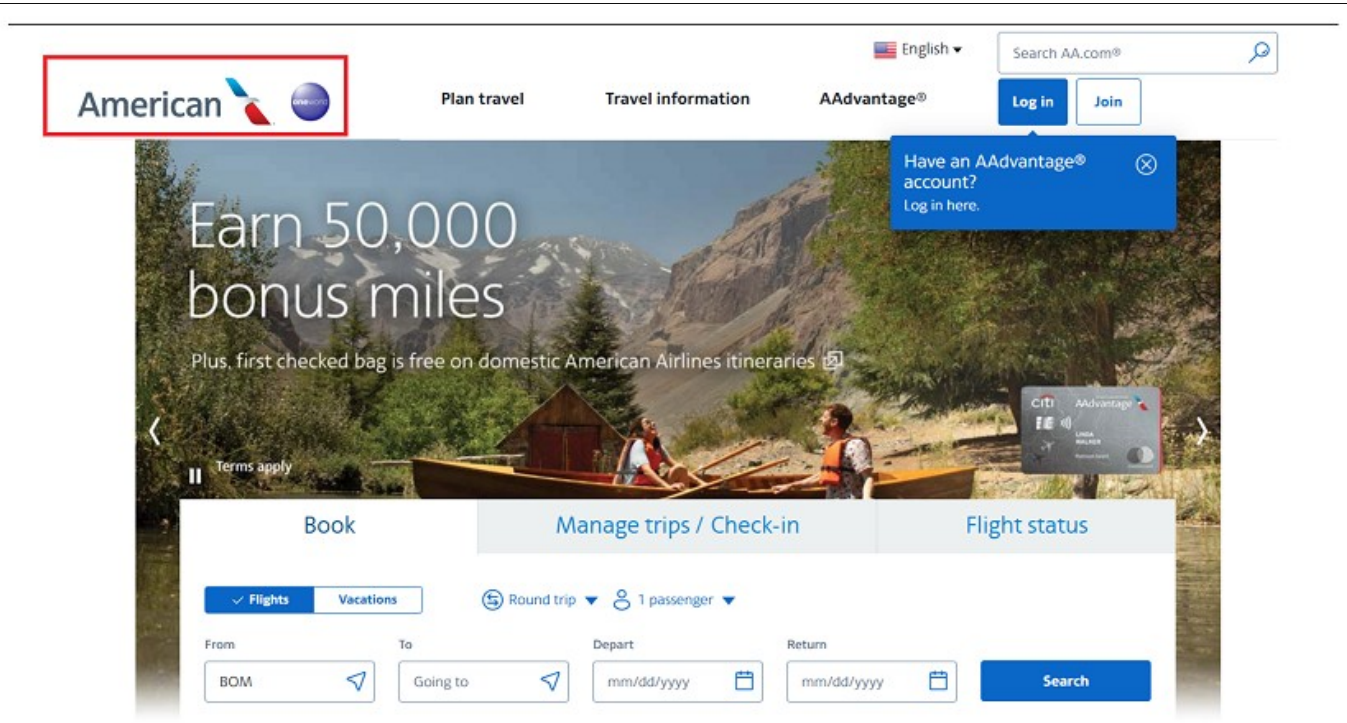
	 Source: Fiddler capture of the accused instrumentality  Source: Fiddler capture of the accused instrumentality
using a processor of the computer system to evaluate, based at least	The accused instrumentality practices using a processor of the computer system (e.g., processor of the authentication server of the accused instrumentality, etc.) to evaluate, based at least on the first signal (e.g., a ROUTEID set response, etc.) and

on the first signal and the second signal, whether the user is authorized to conduct the at least one interaction with the secured capability; and	the second signal (e.g., a request signal from the user device), whether the user is authorized to conduct the at least one interaction (e.g., account login, etc.) with the secured capability (e.g., secure connection with the website, etc.). The server compares the reusable identifier, such as the token (e.g., ROUTEID), in the first response received from the server with the token included in the client's subsequent request. If a match is found, the server authenticates the user and processes the request securely.  Source: Fiddler captures of the accused instrumentality

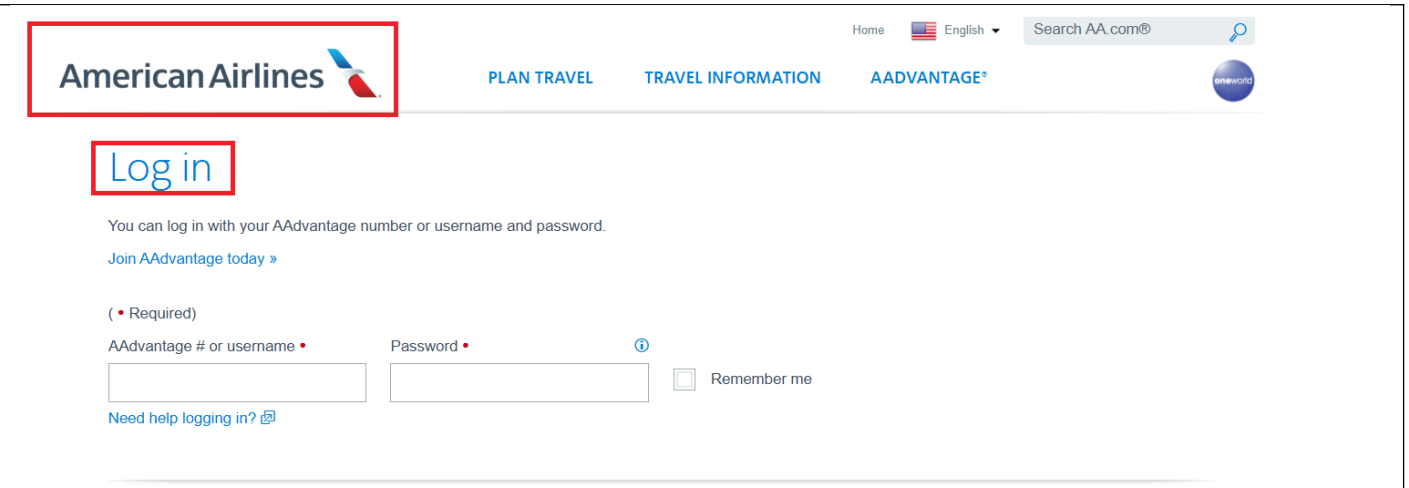


Source: Fiddler Capture of the accused instrumentality

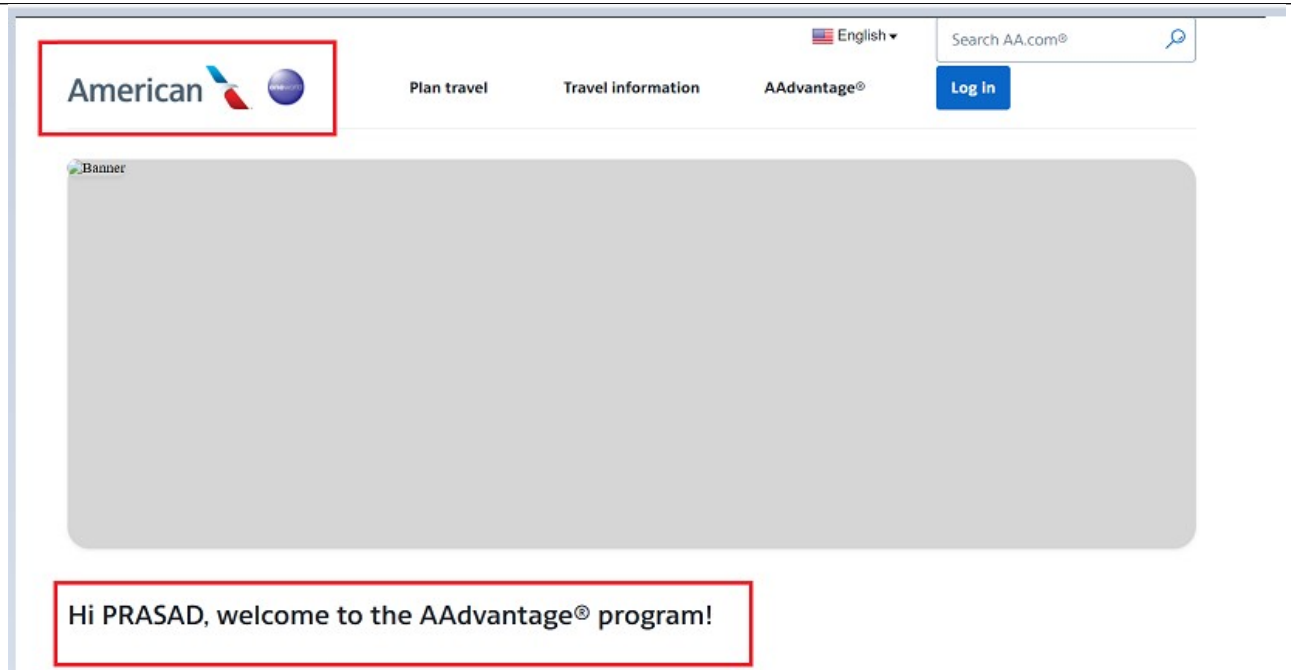
Source: Fiddler capture of the accused instrumentality



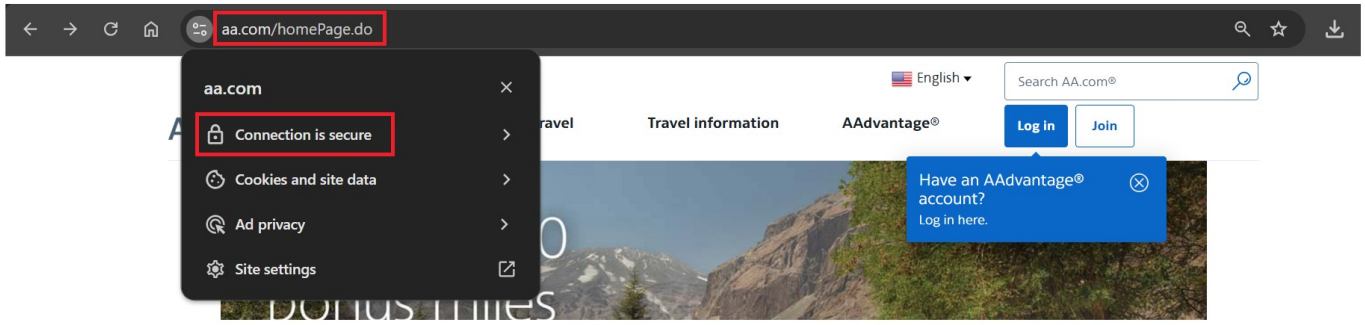
https://www.aa.com/homePage.do



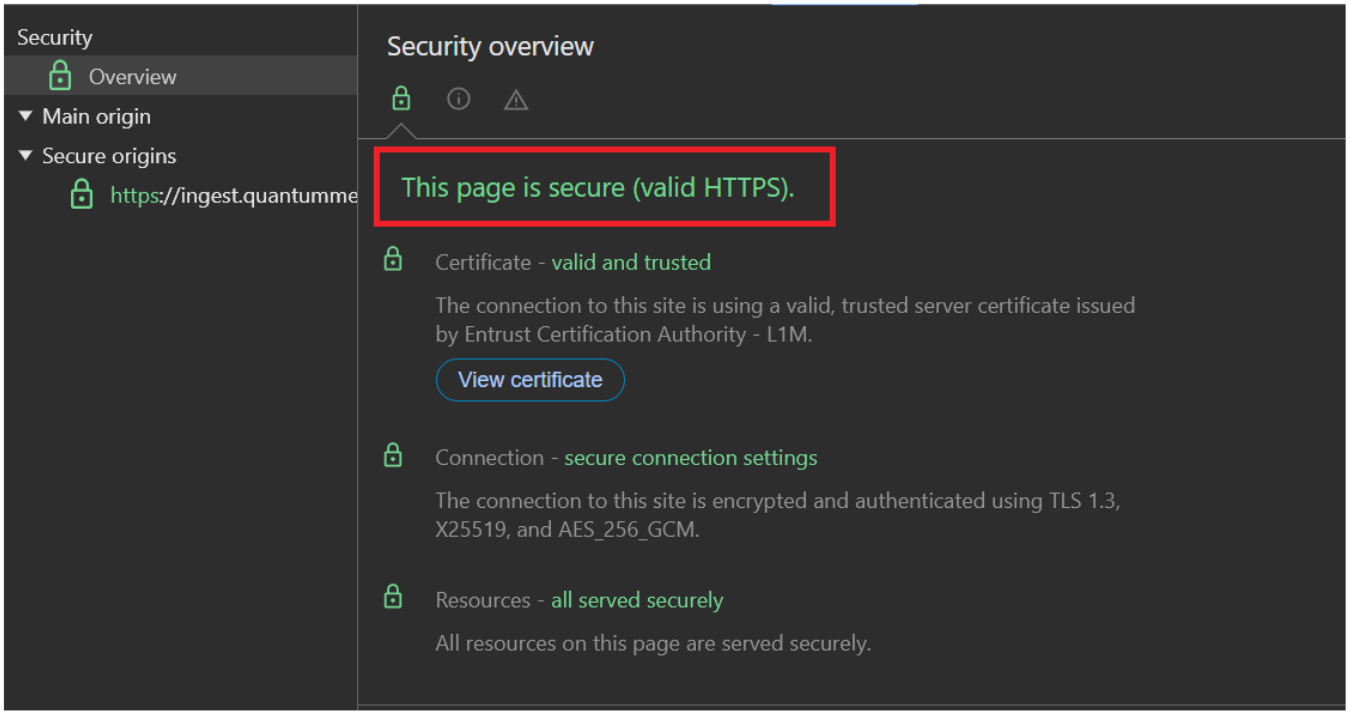
https://www.aa.com/loyalty/login



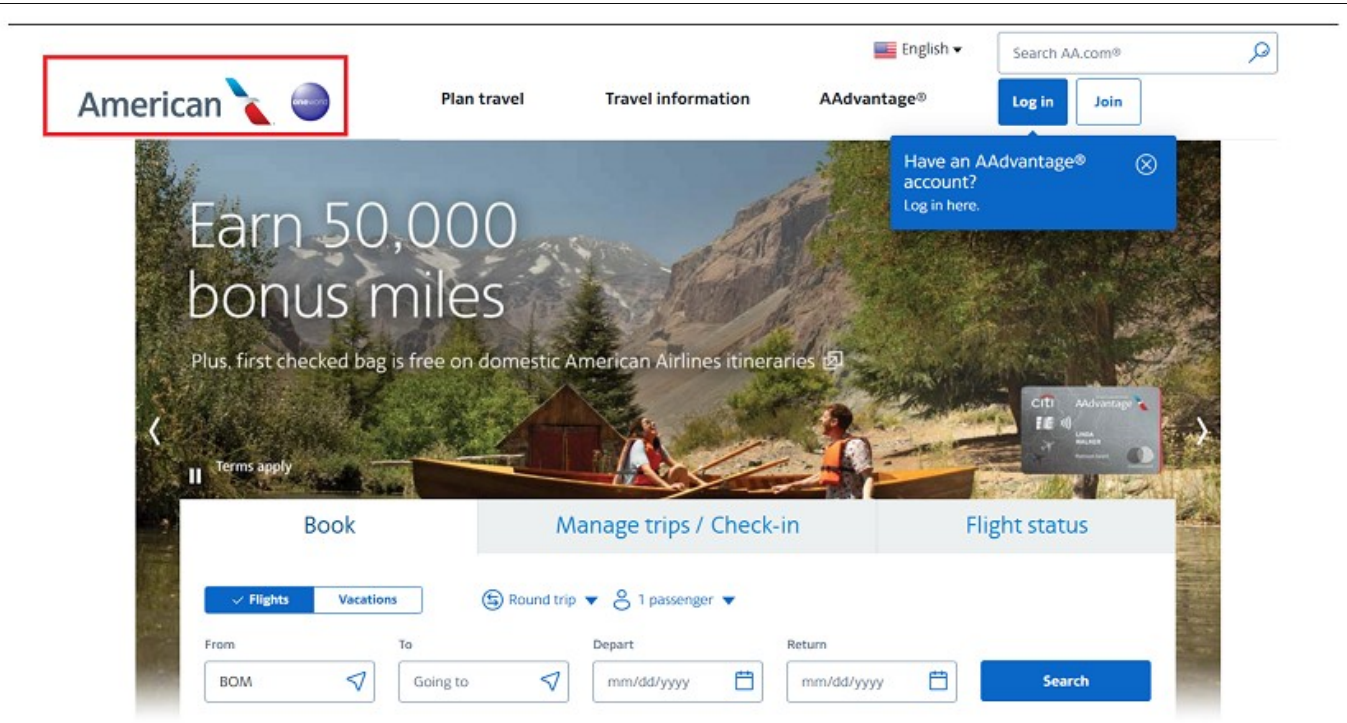
https://www.aa.com/loyalty/login



https://www.aa.com/homePage.do

	 https://www.aa.com/homePage.do
in response to an indication from the processor that the user is authorized to conduct the at least one interaction with the secured capability, using the computer system to transmit a third signal	The accused instrumentality practices in response to an indication from the processor (e.g., processor of the authentication server of the accused instrumentality, etc.) that the user is authorized to conduct the at least one interaction with the secured capability (e.g., secure connection with the website, etc.), using the computer system processor (e.g., authentication server of the accused instrumentality, etc.) to transmit a third signal comprising authorization information (e.g., a response signal from the server to the user device, etc.) to at least one of the electronic device (e.g., user device, etc.) and the computer.

comprising authorization information to at least one of the electronic device and the computer.	As shown, upon authenticating the ROUTEID, the user device receives an authentication confirmation message (a third signal), from the server to the user device.  Source: Fiddler capture of the accused instrumentality



https://www.aa.com/homePage.do